RÈGLEMENT DE POLITIQUE DE SÉCURITÉ

Entreprise : [Nom de l'entreprise]
Adresse : [Adresse complète]
Responsable sécurité / conformité : [Nom]
Version : [Date]

1. Objectif

Ce règlement définit le cadre général de la sécurité dans l'entreprise. Il a pour objectif de protéger les collaborateurs, les visiteurs, les biens matériels, les données sensibles et les systèmes d'information contre tout risque pouvant compromettre leur intégrité, leur disponibilité ou leur confidentialité.

2. Champ d'application

La présente politique s'applique à l'ensemble du personnel, aux prestataires externes, partenaires et visiteurs présents sur les sites de l'entreprise ou ayant accès à ses ressources, physiques ou numériques. Elle couvre la sécurité des personnes, des bâtiments, des équipements, des données et des communications.

3. Sécurité physique

Les locaux de l'entreprise sont sécurisés par des systèmes de contrôle d'accès, d'alarme et de surveillance adaptés à l'activité. L'entrée dans les zones sensibles est réservée aux personnes autorisées. Tout incident (vol, effraction, comportement suspect) doit être signalé immédiatement à la direction ou au responsable sécurité.

4. Sécurité des personnes

L’entreprise s’engage à assurer un environnement de travail sain et sécurisé, conforme à la législation suisse en vigueur (LTr, OLT, SUVA). Chaque collaborateur est tenu de respecter les consignes de sécurité, d’utiliser les équipements de protection nécessaires et de signaler tout danger ou accident. Des formations à la sécurité sont régulièrement dispensées.

5. Sécurité informatique

La sécurité des systèmes informatiques est essentielle à la continuité des activités. Tous les utilisateurs doivent respecter les règles en matière de mots de passe, d’accès aux ressources, de protection contre les logiciels malveillants, et d’usage responsable de l’e-mail et d’internet. Les données sensibles doivent être stockées de manière sécurisée et ne doivent pas être transmises sans autorisation.

6. Protection des données

L’entreprise traite des données personnelles dans le respect de la LPD et, le cas échéant, du RGPD. Toute personne ayant accès à ces données s’engage à respecter leur confidentialité, à ne pas les divulguer et à ne pas les conserver au-delà de la durée légale ou contractuelle. Toute violation doit être immédiatement signalée à la direction ou au DPO.

7. Continuité d’activité et gestion des incidents

Des mesures sont mises en place pour faire face aux situations de crise, telles qu’un sinistre, une attaque informatique ou une panne majeure. Un plan de continuité d’activité est prévu, incluant la sauvegarde régulière des données critiques et la désignation d’une équipe de gestion des incidents. Chaque collaborateur doit connaître les procédures d’urgence applicables.

8. Contrôle, audit et sanctions

Le respect de la politique de sécurité peut faire l’objet de contrôles ou d’audits internes ou externes. Toute violation des règles de sécurité, qu’elle soit volontaire ou par négligence, pourra entraîner des mesures disciplinaires, voire des poursuites judiciaires selon la gravité des faits.

9. Entrée en vigueur et engagement

Ce règlement est remis à chaque collaborateur à son entrée dans l'entreprise. Il doit être lu, compris et signé. L'adhésion à cette politique est une condition d'exercice de toute fonction au sein de l'organisation.

Nom du collaborateur : .....
Fonction : .....
Date : .....
Signature : .....